

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the Email Accounts
[REDACTED] and
[REDACTED],
Maintained at Premises Controlled by
Google, LLC, USAO Reference No.
[REDACTED]

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

20 MAG 022 40

**Agent Affidavit in Support of Application for a Search Warrant
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

[REDACTED] being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption, including wire fraud and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence.

B. The Provider, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the email accounts [REDACTED] ("Subject Account-1") and [REDACTED] ("Subject Account-2") (together, the "Subject Accounts"), maintained and controlled by Google, LLC (the

“Provider”), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (the “Subject Offenses”). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

4. As set forth below, the FBI and U.S. Attorney’s Office for the Southern District of New York (“USAO”) have already obtained a search warrant to search the Subject Accounts for evidence, fruits, and instrumentalities of the Subject Offenses, limited to the time period September 1, 2013 to the present. Based on our initial review of emails obtained pursuant to that warrant, we are now seeking authorization to expand the time period of our search of the Subject Accounts to include content from the date the accounts were created on or about January 29, 2013, through September 1, 2013, *i.e.*, the date of the earliest records obtained through the prior application.

C. Services and Records of the Provider

5. I have learned the following about the Provider:

a. The Provider offers email services to the public. In particular, the Provider permits subscribers to maintain email accounts under the domain name gmail.com or under any domain name under the subscriber's control. For example, if a subscriber controls the domain name "xyzbusiness.com," the Provider enables the subscriber to host any email address under this domain name (e.g., "john@xyzbusiness.com"), on servers operated by the Provider. A subscriber using the Provider's services can access his or her email account from any computer connected to the Internet.

b. The Provider maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Provider's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Provider's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for a certain period of time.

ii. *Address book.* The Provider also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* The Provider collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Provider also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address

of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the Provider maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* The Provider also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider's website).

v. *Google Drive Content.* The Provider provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud" (that is, online). A user can access content stored on Google Drive by logging into his subscriber account through any computer or other electronic device connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

vi. *Google Docs.* The Provider provides users with the ability to write, edit, and collaborate on various documents with other users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive.

vii. *Google Calendar.* The Provider provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered

computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

viii. *Location History.* The Provider maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by the Provider. For example, the Provider collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Provider-1 apps and services also allow for location reporting, which allows the Provider to periodically store and use a device’s most recent location data in connection with a subscriber account.

ix. *Device Information.* The Provider collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

x. *Android Services.* The Provider also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by the Provider, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. The Provider retains information related to the Android device associated with an account, including the IMEI (International Mobile Station Equipment Identifier), MEID (Mobile Equipment Identifier), device ID, and/or serial number of the device. Each of those identifiers

uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

xi. *Cookie Data.* The Provider uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

xii. *Preserved and backup records.* The Provider also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). On or about November 11, 2019, the Government served the Provider with a preservation request for the Subject Accounts. The Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

D. Jurisdiction and Authority to Issue Warrant

6. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

7. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

8. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

9. Attached hereto as Exhibit 1, and incorporated by reference herein, is a search warrant and accompanying affidavit dated December 12, 2019 (19 Mag. 11651) (the “First FG Email Warrant”), which authorized the FBI and USAO to search the Subject Accounts for evidence, fruits, and instrumentalities of the Subject Offenses. The application in support of the First FG Email Warrant sought—and the search warrant authorized—a search of the Subject Accounts limited to the time period September 1, 2013 to the date of the First FG Email Warrant, based on the fact that Fraud Guarantee was incorporated in Delaware in early October 2013. However, as set forth below, the evidence indicates that Parnas and Correia were using the Subject Accounts as early as January 2013, and had solicited at least three investors in Fraud Guarantee (“Early Investor-1,” “Early Investor-2,” and “Early Investor-3”) at least several months earlier than October 2013.

10. Based on my initial review of materials obtained pursuant to the First FG Email Warrant, I have learned the following, in substance and in part:

a. Subscriber information from the Provider reflects that Subject Account-1 (in the name of Parnas) and Subject Account-2 (in the name of Correia) were created on or about January 29, 2013.

b. As of September 2013—*i.e.*, around the time of the earliest results of the First FG Email Warrant—Parnas and Correia were already in discussions with Early Investor-1, Early Investor-2, and Early Investor-3, who appear to have entered into agreements, formal or informal, with Fraud Guarantee prior to that time.

c. For instance, an email chain dated in September 2013 reflects that in late August 2013, Correia (from Subject Account-2), copying Parnas (at Subject Account-1), told Early Investor-1 that Early Investor-1 had already funded \$110,000 of his \$200,000 commitment to Fraud Guarantee, and thus owed the company another \$90,000. Correia instructed Early Investor-1 to wire his funds to an account in the name of “[REDACTED].”

d. Similarly, in a mid-September 2013 email to Early Investor-2, Correia (from Subject Account-2), copying Parnas (at Subject Account-1) referred to “\$50k you are sending in this week” and attached a Convertible Note issued by [REDACTED], a Florida limited liability company, in the amount of \$100,000, dated May 9, 2013, and signed by Correia.

11. Based on my review of documents produced by the Florida Department of State, I have learned that [REDACTED] was incorporated in Florida on or about November 30, 2012, with Correia listed as the managing member.

12. Based on my review of documents obtained from Early Investor-3, I have learned the following, in substance and in part: A confidentiality agreement between Parnas, in his capacity as “Director and Chief Executive Officer” of [REDACTED], and Early Investor-3, was signed by Early Investor-3 and dated January 21, 2013. On or about the same date, Correia sent a letter to Early Investor-3, “[o]n behalf of [REDACTED] (d/b/a [FraudGuarantee.com]),” in which Correia offered Early Investor-3 a “\$150,000 convertible debenture with an[] 8% annualized return, to be converted at 1.5% in the company.”

13. In sum, it appears that prior to incorporating Fraud Guarantee in Delaware in or about early October 2013, Parnas and Correia were operating the company through the entity [REDACTED] and using the Subject Accounts to do so. In particular, it appears that Parnas's and Correia's discussions with potential investors took place at least as early as January 2013, which is approximately the same time the Subject Accounts were created.

14. Accordingly, there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses exist within the Subject Accounts from the date the accounts were created (on or about January 29, 2013), to the date of records obtained pursuant to the First FG Email Warrant (September 1, 2013). Such evidence likely includes correspondence between Parnas and Correia concerning their plans for soliciting investments to Fraud Guarantee, and/or regarding the actual or anticipated operations of Fraud Guarantee (or lack thereof); and correspondence with actual and potential investors in the company, including any materials concerning Fraud Guarantee's actual or projected operations, finances, strategy, or leadership. Such material would provide evidence as to the nature of Parnas's and Correia's representations to potential investors during the 2013 time period, and would reveal whether Parnas and Correia were engaged in fraudulent misrepresentations at that time. Such evidence would also reveal the amount of funds obtained from investors in the 2013-15 time period, and the use of such funds, which would provide evidence regarding the falsity or truthfulness of various representations made by Parnas and Correia in the 2015-18 time period concerning how much money Fraud Guarantee had raised to that point, and how such funds had been used.

15. Furthermore, based on my training and experience, and consistent with the pattern of communications reflected in Exhibit 1, I know that individuals who communicate via text or WhatsApp typically also communicate about the same subjects via email.

16. Additionally, based on my training and experience, email accounts like the Subject Accounts, which have been used to communicate with others in furtherance of the Subject Offenses often contain records of that activity, including email correspondence, address books with contact information for co-conspirators, and documents saved as email attachments or to Google Docs or Google Drive folders.

17. Additionally, based on my training and experience, and my participation in this investigation, it appears that Parnas and Correia had various meetings with actual or potential investors and partners in Fraud Guarantee, and that evidence in the Subject Accounts will corroborate the existence of such meetings. Specifically, location data, IP transaction records, and calendar entries may contain evidence to establish the location of Parnas, Correia, or others at relevant dates set forth above. Furthermore, device information, and cookie data for linked accounts, may contain evidence of other email accounts or electronic devices that could contain evidence of the Subject Offenses, including correspondence with co-conspirators or location information to corroborate the existence of meetings. Indeed, from my participation in this investigation, I have learned that the individuals involved in the commission of the Subject Offenses have used multiple email or iCloud accounts, and/or multiple cellphones, to communicate with co-conspirators.

18. Temporal Limitation. This application is limited to all content created, sent, or received from the date that the Subject Accounts were created (on or about January 29, 2013), through September 1, 2013.

A. Evidence, Fruits and Instrumentalities

19. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Accounts will contain

evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

20. In particular, I believe the Subject Accounts are likely to contain the following information:

a. Evidence relating to, including communications with, any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to false and fraudulent representations made to potential or actual investors, including drafts of any corporate documents and related materials;

e. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

f. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

g. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

h. Evidence of meetings between Parnas, Correia, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

i. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

j. Passwords or other information needed to access user's online accounts.

III. Review of the Information Obtained Pursuant to the Warrant

21. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

22. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as

searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

23. While Parnas, Correia, and others have been publicly indicted with respect to separate charges, and there has been some public reporting about the existence of an investigation into the removal of Ambassador [REDACTED], the scope and focus of this aspect of the criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert criminal targets to the scope and focus of the investigation, causing them to destroy evidence, tamper with witnesses, or otherwise seriously jeopardize the investigation. Specifically, from my experience investigating public corruption offenses, I know that individuals who participate in offenses such as the Subject Offenses may communicate about known government investigations and tailor their stories to be consistent, and tamper with or hide potential evidence. Accordingly, premature disclosure of the scope of this investigation would undermine efforts to obtain truthful statements from relevant witnesses, and could lead to witness tampering and/or obstruction of justice. In addition, if the subjects of this investigation were alerted to the existence of a criminal investigation, it may prompt them to delete electronic records, including in e-mail accounts or other electronic media not presently known to the government. Accordingly, there is reason to believe that, were the Provider to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized.

24. Additionally, while the Subject Accounts are registered to an enterprise domain (fraudguarantee.com), there is no representative of the enterprise that could be notified without

seriously jeopardizing the investigation. Indeed, as described above, the subscribers of the Subject Accounts are the CEO and COO of the enterprise, the enterprise itself appears to be an instrumentality of the fraudulent scheme, and there is no known employee of the enterprise or a legal representative that could be notified without jeopardizing the investigation. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person, including any representative of the enterprise domain fraudguarantee.com, of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

25. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

26. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C.

§ 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.



Sworn to before me this
__th day of February, 2020

A handwritten signature in black ink, appearing to read "J. Paul Oetken".

HONORABLE J. PAUL OETKEN
United States District Judge
Southern District of New York



EXHIBIT 1

19 MAG 11 65 1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the Email Accounts
[REDACTED] and
[REDACTED]
Maintained at Premises Controlled by
Google, LLC, USAO Reference No.
[REDACTED]

TO BE FILED UNDER SEAL
AGENT AFFIDAVIT

Agent Affidavit in Support of Application for a Search Warrant
for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

[REDACTED], being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption, including wire fraud and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence.

B. The Provider, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the email accounts [REDACTED] ("Subject Account-1") and [REDACTED] ("Subject Account-2") (together, the "Subject Accounts"), maintained and controlled by Google, LLC (the

"Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (the "Subject Offenses"). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

4. I have learned the following about the Provider:

a. The Provider offers email services to the public. In particular, the Provider permits subscribers to maintain email accounts under the domain name gmail.com or under any domain name under the subscriber's control. For example, if a subscriber controls the domain name "xyzbusiness.com," the Provider enables the subscriber to host any email address under this domain name (e.g., "john@xyzbusiness.com"), on servers operated by the Provider. A subscriber using the Provider's services can access his or her email account from any computer connected to the Internet.

b. The Provider maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Provider's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Provider's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for a certain period of time.

ii. *Address book.* The Provider also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* The Provider collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Provider also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the Provider maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* The Provider also typically retains certain transactional information about the use of each account on its system. This information can include records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider's website).

v. *Google Drive Content.* The Provider provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can

purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud” (that is, online). A user can access content stored on Google Drive by logging into his subscriber account through any computer or other electronic device connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

vi. *Google Docs.* The Provider provides users with the ability to write, edit, and collaborate on various documents with other users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

vii. *Google Calendar.* The Provider provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

viii. *Location History.* The Provider maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by the Provider. For example, the Provider collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Provider-1 apps and services also allow for location reporting, which allows the Provider to periodically store and use a device’s most recent location data in connection with a subscriber account.

ix. *Device Information.* The Provider collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts,

including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

x. *Android Services.* The Provider also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by the Provider, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. The Provider retains information related to the Android device associated with an account, including the IMEI (International Mobile Station Equipment Identifier), MEID (Mobile Equipment Identifier), device ID, and/or serial number of the device. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

xi. *Cookie Data.* The Provider uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

xii. *Preserved and backup records.* The Provider also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon

receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). On or about November 11, 2019, the Government served the Provider with a preservation request for the Subject Accounts. The Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

D. Jurisdiction and Authority to Issue Warrant

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

Overview

8. On or about October 9, 2019, a grand jury sitting in the Southern District of New York returned an indictment charging defendants Lev Parnas and Igor Fruman with conspiring to make

contributions in connection with federal elections in the names of others, in violation of 18 U.S.C. § 371 and 52 U.S.C. §§ 30122 and 30109; and with making false statements and falsifying records to obstruct the administration of a matter within the jurisdiction of the Federal Election Commission, in violation of 18 U.S.C. §§ 1001 and 1519. Additionally, the same indictment charges Parnas, Fruman, David Correia, and Andrey Kukushkin with conspiring to violate the ban on foreign donations and contributions in connection with federal and state elections, in violation of 18 U.S.C. § 371 and 52 U.S.C. §§ 30121, 30122, and 30109.

9. In addition to prosecuting Parnas, Fruman, Correia, and Kukushkin for the above-referenced crimes, the FBI and U.S. Attorney's Office for the Southern District of New York ("USAO") are investigating, among other things, whether Parnas and Correia, and others known and unknown, perpetrated a fraudulent scheme through their efforts to raise funds ostensibly for their business "Fraud Guarantee," in violation of 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt/conspiracy to commit the same). In sum, and as described below, the evidence provides probable cause to believe that Parnas and Correia solicited multiple investors to contribute hundreds of thousands of dollars to Fraud Guarantee based on materially false explicit and implicit representations regarding the Fraud Guarantee business, including its finances, leadership, and relationship with Rudolph Giuliani and his firm, [REDACTED].

Probable Cause as to the Wire Fraud Scheme

10. Based on my review of records obtained from the State of Delaware, Division of Corporations, I have learned that (i) "Fraud Guarantee, LLC" was registered in Delaware on or about October 4, 2013, and that corporate registration was cancelled by Delaware on or about June 1, 2018 "by reason of its neglect, refusal, or failure to pay its annual taxes"; and (ii) "Fraud Guarantee Holdings, LLC" was registered in Delaware on or about February 22, 2016, and "ceased

to be in good standing on [June 1, 2019] by reason of neglect, refusal, or failure to pay an annual tax.”

11. According to the Fraud Guarantee website (fraudguarantee.com), Parnas is listed as the Co-Founder and CEO, and Correia is listed as the Co-Founder and COO of the company. The website describes Fraud Guarantee as a company that “help[s] reduce the risk of fraud as well as mitigate the damage caused by fraudulent acts . . . by building products that protect investors in the private equity marketplace,” and states that “Fraud Guarantee provides . . . investors peace of mind through comprehensive intelligence, and insurance against losses due to fraudulent behavior, or defaults due to fraud.” The website states that Fraud Guarantee’s “InvestSafe” product “is expected to launch in Spring 2016” and “[i]s an insurance product which will insure investors against investment fraud.” It further states that “Fraud Guarantee provides best of breed technology with respect to background check and due diligence products” and “also offer[s] a new product that does not currently exist in the industry today.”

12. Based on my discussions with four individuals who invested in Fraud Guarantee and/or their counsel (“Victim-1,” “Victim-2,” “Victim-3,” and “Victim 4”), my discussion with an individual who served as Chief Executive Officer of Fraud Guarantee (the “CEO”), my review of documents produced by the foregoing individuals, my review of financial records, and my participation in this investigation, I have learned the following, in substance and in part:

a. On or about September 6, 2015, Correia emailed a potential investor (Victim-1) and stated, in sum, that Fraud Guarantee would be raising \$3 to \$5 million in capital, and was offering a “small piece to our friends and family network at a \$20 million dollar valuation,” noting that the next round of capital would be raised “at a \$30,000,000 to \$50,000,000 valuation, thus, a

discount to our close network.” Correia said that “[d]ue to the significant demand we have . . . we are only able to offer \$300,000 at this time.”

i. Based on my discussions with the CEO and my review of Parnas’s and Correia’s correspondence, as well as financial records and other documents, it does not appear that Fraud Guarantee had any significant impending investment at this time, much less one in the range of \$3 to \$5 million. Nor is it clear on what basis Parnas and Correia ascribed a \$20 million valuation—or \$30 to \$50 million valuation—to Fraud Guarantee which, at this time, appears to have had no viable products, no customers, no revenue, no sales, no employees, and at most *de minimus* assets.

ii. Correia attached two documents to his email to Victim-1: a Fraud Guarantee business plan (the “Business Plan”) and a proposed Convertible Loan Agreement. The Business Plan began with an introduction signed by Parnas which stated that “[t]he market we are entering exceeds \$1 Trillion on an annual basis,” and that “[w]e project to obtain 2% of this market, a highly conservative estimate, due to the complete lack of competition. Gaining this market share equates to over \$60 Million in revenue by year three. This business plan has been prepared to provide investors with the information necessary to make an informed investment decision.”

iii. The Business Plan stated that Parnas, the Founder and CEO of Fraud Guarantee, “founded a brokerage firm that eventually became the fifth largest wholesale-market maker in the United States, employing over 200 traders. Mr. Parnas’ firm made markets for over 4,500 stocks, and took over 1000 companies public.” Based on my involvement in this investigation and review of publicly available information, this statement appears to be false. Records in the public domain reflect that Parnas previously worked for three stock brokerage firms, each of which was expelled by the Financial Industry Regulatory Authority (FINRA) for fraud or

other violations. The Business Plan further stated that Parnas “align[ed]” with “an emerging technology company” and “took it public, ultimately realizing a \$600MM market cap.” Based on my review of public records, I have identified no evidence of Parnas assisting any company in achieving an Initial Public Offering (IPO) or obtaining a \$600 million market capitalization. The Business Plan also made various assertions about Correia’s professional history—for example, that he “has built, operated and sold several companies”—that appear, based on my review of publicly available documents, to be gross exaggerations if not falsehoods.

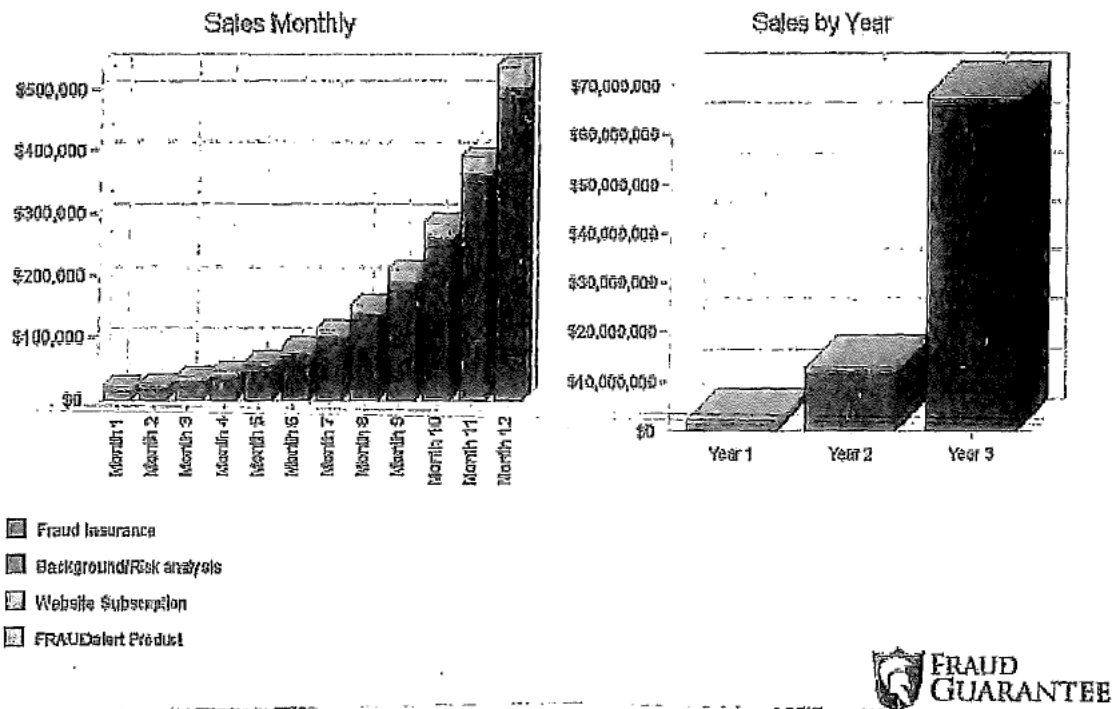
iv. The Business Plan described the “Original Seed Capital Budget” as follows:

Original Seed Capital Budget	
Already accomplished	
Start-up Expenses	\$1,500
Legal	\$5,000
Insurance	\$15,000
Meals and Entertainment	\$3,000
Utilities	\$12,000
Accounting	\$25,000
Travel Expense	\$50,000
Lobbying	\$12,000
Admin payroll	\$10,000
Web development	\$5,000
FF+E	\$26,500
Office lease	\$800
Supplies	\$3,000
IT support	\$167,305
Total Start-up Expenses	
Start-up Assets	
Cash Required	\$100,000
Start-up Inventory	\$0
Other Current Assets	\$0
Long-term Assets	\$25,000
Total Assets	\$125,000
Long-term Assets	\$25,000
Total Assets	\$125,000
Total Requirements	\$292,305

Although the Business Plan stated that these financing needs were “[a]lready accomplished,” based on my review of financial records and correspondence, it does not appear that Fraud Guarantee even maintained a bank account at this time; and based on my discussions with the CEO, I understand that he is not aware of any Fraud Guarantee funds having been used to cover such expenses.

v. The Business Plan provided a sales forecast as follows, despite the fact that, as noted above, it does not appear that Fraud Guarantee had any viable products or customers at this time, and had not reached an agreement with an insurance carrier to back any of the products it hoped to bring to market:

Sales Forecast	Year 1	Year 2	Year 3
Sales			
Fraud Protection	\$1,670,827	\$11,430,887	\$66,000,000
Background/Risk analysis	\$128,310	\$953,334	\$1,040,000
Website Subscription	\$0	\$42,755	\$680,540
FRAUDalert Product	\$178,105	\$532,174	\$585,000
Total Sales	\$1,977,242	\$12,959,150	\$68,305,540
Direct Cost of Sales			
Fraud protection Rev-Share	\$334,167	\$2,286,177	\$13,200,000
Background check/risk analysis	\$10,706	\$88,085	\$99,753
Subscription/Membership	\$0	\$0	\$0
FRAUDalert	\$0	\$0	\$0
Subtotal Direct Cost of Sales	\$344,873	\$2,374,262	\$13,299,753



vi. The Business Plan stated that Fraud Guarantee was seeking to raise at least approximately \$3.5 million, which “Mr. Parnas believes . . . can be completed no later than April 1st, 2015.”

vii. The Business Plan provided the following description of how the approximately \$3.5 would be spent:

Start-up Funding	
	Year 1
Sales	\$1,977,242
Direct Cost of Sales	\$344,873
Other Costs of Sales	\$34,805
Total Cost of Sales	\$379,678
Gross Margin	\$1,597,564
Gross Margin %	80.80%
Expenses	
Payroll	\$1,431,070
Marketing/Promotion	\$290,024
Depreciation	\$0
Rent	\$55,500
Utilities	\$6,000
Insurance	\$5,400
Payroll Taxes	\$214,661
Website development/SEO	\$75,000
Computers/Technology	\$30,000
FP&E	\$24,000
Meals and Entertainment	\$102,000
Accounting	\$49,992
Travel Expense	\$300,000
Consulting	\$150,000
Lobbying/political donations	\$120,000
Marketing materials	\$24,995
Health Insurance	\$75,000
Risk analysis tool Investment	\$150,000
Captive build-out	\$500,000
Total Operating Expenses	\$3,603,643

viii. The Business Plan stated that Fraud Guarantee “expects to continue its steady growth in profitability over the next three years of operation,” and projected as follows:

Pro Forma Profit and Loss	Year 1	Year 2	Year 3
Sales	\$1,977,242	\$12,059,150	\$68,305,540
Direct Cost of Sales	\$344,873	\$2,374,262	\$13,299,753
Other Costs of Sales	\$24,805	\$259,183	\$1,366,110
Total Cost of Sales	\$379,678	\$2,633,445	\$14,665,863
Gross Margin	\$1,597,564	\$10,325,705	\$53,639,677
Gross Margin %	80.80%	79.68%	78.53%
Expenses			
Payroll	\$1,421,070	\$1,928,434	\$2,530,139
Marketing/Promotion	\$290,024	\$500,000	\$700,000
Depreciation	\$0	\$0	\$0
Rent	\$53,500	\$57,000	\$58,720
Utilities	\$6,000	\$6,500	\$7,000
Insurance	\$5,400	\$5,800	\$6,200
Payroll Taxes	\$214,661	\$289,265	\$349,521
Website development/SBO	\$75,000	\$50,000	\$70,000
Computers/Technology	\$30,000	\$10,000	\$10,000
FF&E	\$24,000	\$5,000	\$5,000
Meals and Entertainment	\$102,000	\$120,000	\$150,000
Accounting	\$49,692	\$60,000	\$70,000
Travel Expense	\$300,000	\$400,000	\$500,000
Consulting	\$150,000	\$170,000	\$190,000
Lobbying/political donations	\$20,000	\$200,000	\$250,000
Marketing materials	\$24,996	\$40,000	\$50,000
Health Insurance	\$75,000	\$80,000	\$85,000
SEP White Investment	\$450,000	\$0	\$0
Insurance product build-out	\$200,000	\$0	\$0
Total Operating Expenses	\$3,603,643	\$3,921,999	\$4,831,589
Profit Before Interest and Taxes	(\$2,006,079)	\$6,403,706	\$48,808,097
EBITDA	(\$2,006,079)	\$6,403,706	\$48,808,097
Interest Expense	\$0	\$0	\$0
Taxes Incurred	\$0	\$1,921,112	\$14,642,429
Net Profit	(\$2,006,079)	\$4,482,594	\$34,165,668
Net Profit/Sales	-101.46%	34.59%	50.02%

ix. The Business Plan provided various other financial projections, including a “pro forma balance sheet” which showed “strong profits beginning in year two.”

b. On or about October 20, 2015, Correia, copying Parnas, emailed Victim-1 a Convertible Loan Agreement. The agreement was signed by Parnas and provided that Victim-1 (through his entity) would provide a \$300,000 loan to Fraud Guarantee, which could be converted

into equity in the company, "to be used . . . to finance the development, promotion and initial operation of an investment protection business known as 'Fraud Guarantee.'" The agreement further stated that "[t]he purpose of the Loan is to provide funds for certain approved costs for the development, staffing, promotion, sales and marketing arrangements, and operation of the Business . . . The Loan shall be fully reserved and committed for the costs to complete the funding of the Business Investment with proceeds of the Loan." The agreement provided for a maturity date of October 19, 2017. The agreement also provided that Fraud Guarantee represented, among other things, that "[a]ll information furnished to [Victim-1] regarding the financial status of [Fraud Guarantee] will be, at the time the same are so furnished, accurate and correct in all material respects and complete insofar as completeness may be necessary to give [Victim-1] a true and accurate knowledge of the subject matter." At some point thereafter, Victim-1 signed the agreement.

c. On or about December 1, 2015, Parnas, copying Correia, emailed Victim-1 with the subject line, "Wire info." Parnas provided the bank information for an account in the name of [REDACTED] (the [REDACTED] Account") and indicated that the wire was for "[r]epayment of loan to satisfy investment info Fraud Guarantee." Based on my review of bank records, I have learned that Parnas was the sole signatory on the [REDACTED] Account, and that this account was used by Parnas personally, not by Fraud Guarantee. On or about the same day, Victim-1 emailed Correia to confirm that he had wired the first payment "to [the [REDACTED] Account] who paid the 300000\$ to [F]raud [G]uarantee." Accordingly, it appears that Parnas told Victim-1 that he (Parnas) had paid \$300,000 to Fraud Guarantee to cover Victim-1's forthcoming investment, and that Victim-1 should thus repay the "loan" to Parnas directly via the [REDACTED] Account. As noted above, however, it does not appear that Fraud Guarantee even maintained a

bank account at this time. Further, based on my discussions with the CEO, I understand he is not aware of Parnas contributing any money—much less \$300,000—to Fraud Guarantee at or around this time.

d. On or about December 9, 2015, Victim-1 asked Correia for an update regarding, among other things, Fraud Guarantee's effort to reach a deal with an insurance carrier—a necessary prerequisite for the company to offer its insurance product—and Fraud Guarantee's effort to obtain a multimillion-dollar grant from the Consumer Financial Protection Bureau ("CFPB"). Correia responded that, with respect to the insurance carrier, he was "finalizing all of the information they need to move to a final agreement," which was a "tedious process and can take another couple of weeks"; and with respect to the grant application: "We should have first draft of application for the CFPB by tomorrow afternoon and most likely will submit final application by Monday of next week. We already have one of three congressman on board, [REDACTED] (R) from Mississippi. We should have [REDACTED] (D) from New York and senator [REDACTED] (R) from Alabama on board by Monday the latest. . . . Assuming all goes well, and everything is pointing that way, we could receive funding as early as early February."

e. On or about December 30, 2015, Victim-1 emailed Parnas to confirm that he received his wire payment, and Parnas confirmed. Based on my review of financial records, I have learned that Victim-1 continued to wire money to the [REDACTED] Account in installments from in or about January 2016 to in or about May 2016, noting that each wire constituted a partial repayment of a "loan" to satisfy his investment into Fraud Guarantee. Financial records further reflect that after these funds were wired into the [REDACTED] Account, Parnas used them for predominantly personal purposes, such as restaurants, hotels, and retail stores; and also transferred approximately \$5,500

to Correia's wife. Records do not reflect that any of the funds were used for the purposes set forth in the Business Plan that had been sent to Victim-1. *See supra* ¶ 12(a)(vii).

f. On or about March 18, 2016, Correia, copying Parnas, emailed Victim-1 and attached documentation providing that (i) Victim-1's agreement with Fraud Guarantee, pursuant to which he received 1.5% equity in exchange for \$300,000, would be terminated, and (ii) in its place, Victim-1 would enter into a transaction directly with Parnas, pursuant to which the same \$300,000 would result in Victim-1 receiving 3% equity in the company. It does not appear that this transaction served any legitimate business purpose, apart from providing a *post hoc* justification for the fact that Victim-1 had wired his "investment" to Parnas directly (via [REDACTED] Account). Furthermore, by structuring the transaction as a direct equity sale between Parnas and Victim-1, the contract no longer contained representations regarding how the funds would be used by Fraud Guarantee. As noted below, Parnas and Correia used the same structure with subsequent victim "investors."

g. On or about March 21, 2016, Parnas exchanged emails with a new potential investor (Victim-2), in which Parnas and Victim-2 agreed, in sum, that Parnas would provide Victim-2's entity with a 2.5% equity stake in Fraud Guarantee in exchange for the equivalent of \$250,000—comprised of \$115,000 plus a 2009 Nissan GTR, a 2014 Toyota Tacoma, and a 2004 Jeep Wrangler. On or about two days later, Victim-2 emailed Correia to confirm that "Lev [Parnas] has received payment." On or about six days later, Correia, copying Parnas, sent Victim-2 certain Fraud Guarantee corporate documents, one of which reflected that Parnas, as a member of Fraud Guarantee, had a "capital account" of \$570,000. However, based on my review of financial records, I have identified no evidence of Parnas contributing \$570,000 to Fraud Guarantee, nor

any evidence that Fraud Guarantee had any *non-de minimis* assets at this time. Indeed, as noted above, it does not appear that Fraud Guarantee had even opened a bank account by this point.

h. On or about April 19, 2016, Correia, copying Parnas, sent Victim-2 a signed agreement finalizing the deal for Parnas to sell a 2.5% equity stake in Fraud Guarantee in exchange for \$250,000 from Victim-2. This email attached another copy of the Fraud Guarantee Operating Agreement, reflecting that Parnas had a "capital account" of \$570,000.

i. Based on my review of financial records, I have learned that Victim-2's entity transferred funds to an account in the name of Parnas and his wife in multiple installments between in or about January 2016 and in or about June 2016, noting each time that the funds were to be used to purchase equity in Fraud Guarantee. Financial records further reflect that Parnas and his wife used these funds for predominantly personal purposes, including withdrawing thousands of dollars in cash and transferring thousands of dollars to Correia's wife.

j. On or about May 4, 2016, Fraud Guarantee's CEO emailed Parnas and Correia regarding his employment agreement. The CEO had been hired as of September 15, 2015, pursuant to an agreement which entitled him to an annual salary of \$250,000, paid bi-monthly. Emails and other documents reflect that, since that time, the CEO had worked on various Fraud Guarantee projects. In this email to Parnas and Correia, the CEO complained that he was owed \$180,958.20 in back wages, and provided certain options for him to be paid "[u]pon receipt of any funding."

k. Also on or about the same day, the CEO, copying Correia, contacted a bank in regard to opening an account for Fraud Guarantee. On or about May 26, 2016, the CEO informed Parnas and Correia that the account had been opened and would "provide us with all of our required banking needs now and as we grow." Based on my discussions with the CEO, I have learned that

although he assumed that Fraud Guarantee must have had a bank account prior to that point, he never saw any evidence of it.

1. On or about October 10, 2016, Correia, copying Parnas, emailed a new potential investor (Victim-3) attaching a proposed agreement whereby Parnas would sell 300,000 units of Fraud Guarantee—representing “3% of the outstanding membership interests of the [c]ompany”—to Victim 3, in exchange for \$300,000. Correia, copying Parnas, also sent Victim-3 various Fraud Guarantee corporate documents, including the company’s “Business Plan.” This version of the Business Plan was largely the same as the one previously sent to Victim-1—including making essentially the same apparently false and baseless representations regarding Parnas, Correia, and the company (*see supra* ¶¶ 12(a)(ii) – (ix))—except that it no longer stated that the \$292,305 “Original Seed Capital Budget” was “already accomplished.”

m. On or about the next day, Victim-3 (through his agent) asked Correia to identify the “active members of the LLC (names and percentages), as well as the current value of the LLC, if any.” In response, Correia wrote that Victim-3 “is buying in at a \$10M valuation.” Correia also attached the Fraud Guarantee Operating Agreement, noting that it “shows the members and number of units owned.” In a follow-up email, Correia told Victim-3 that although the “Cap Table of the operating agreement [states] that the capital contributions for all member are only \$100,” “[t]his was done simply to create a cost basis going into this new entity” since “[w]e were previously in a different entity and migrated into what is now Fraud Guarantee Holdings, LLC. There was ‘significant’ investment from all parties in order to take ownership. Is equated to several millions of dollars invested.” Based on my discussions with the CEO, I understand that although Parnas told him that he (Parnas) had invested “millions” in Fraud Guarantee, the CEO never saw

any evidence of such funds, and indeed, saw no evidence of a Fraud Guarantee bank account until he opened one in May 2016.

n. On or about October 14, 2016, Victim-3 returned the signed agreement, and wired \$300,000 to the [REDACTED] Account pursuant to Parnas's and Correia's directions.¹ Financial records reflect that after these funds were received by the [REDACTED] Account, Parnas used them for predominantly personal purposes, including transferring approximately \$160,000 to an account in his and his wife's name (of which, \$25,000 was transferred to Correia's wife), withdrawing approximately \$19,000 in cash, and spending thousands of dollars on restaurants and retail stores.

o. On or about November 12, 2016, Correia, copying Parnas, emailed a new potential investor ("Intended Victim-1"), attaching a proposed agreement "for the transaction you are executing." The proposed agreement provided for Intended Victim-1 to pay \$1 million to Parnas (via the [REDACTED] Account) in exchange for 1,000,000 units of Fraud Guarantee, "represent[ing] 10% of the outstanding membership interests of the [c]ompany." Correia, copying Parnas, also sent Intended Victim-1 various Fraud Guarantee documents, including the Business Plan—which, as noted above, contained multiple apparently false and baseless representations and projections about the company (*see supra* ¶¶ 12(a)(ii) – (ix)).

p. Intended Victim-1 ultimately decided not to invest in Fraud Guarantee. On or about February 11, 2017, Intended Victim-1 forwarded Victim-3 an email from Correia (copying Parnas)

¹ In prior search warrant affidavits, the FBI asserted that there was probable cause to believe that Victim-3's \$300,000 payment was intended by Victim-3 to cover the cost of Parnas's and Correia's donations to [REDACTED] PAC. *See, e.g.*, 19 Mag. 7594; 19 Mag. 8274. However, as set forth herein, having now spoken with Victim-3 and reviewed documents produced by him, Victim-3 has indicated that he had no knowledge his funds would be used to cover the cost of any political donation and there is thus probable cause to believe that Victim-3 was defrauded as part of the scheme described herein and did not intend for his investment to cover the cost of any political donations.

in which they purported to “cancel[]” the purchase agreement. Intended Victim-1 said to Victim-3, “He called me a about fraud GUARANTEE and went ballistic . . . , Evidently he thought I was still giving him a million bucks. He said I can't believe you signed the papers and he made a big change in his company to help me get 10% of his business like he was doing me a great favor. He said he had to convince the board and all that bullshit to get me those shares. He basically forced me to sign on my plane because he told me it had to be done by a certain date and I told him I never invest in anything unless I love it. Obviously he didn't get that part.”

q. On or about February 24, 2017, the CEO—who, as noted above, had emailed Parnas and Correia in or about May 2016 regarding back-owed wages of \$180,958.20 (*see supra* ¶ 12(j))—emailed Parnas and Correia to follow up concerning his “continued, defaulted employment / equity agreement.” The CEO stated that he was now owed \$404,494.80 in “unpaid salary and benefits starting from my hiring date — September 15, 2015 to present.”

r. On or about June 6, 2017, Victim-3's counsel transmitted a letter to Parnas, Correia, and the CEO (the “Demand Letter”), in which he stated that “[s]ince his investment last year, [Victim-3] has not received any of the information required by [certain sections of Fraud Guarantee's Operating Agreement], nor has he received any of the information required by [certain provisions of Delaware law],” and demanded certain specific information. On or about June 13, 2017, Correia sent the CEO draft responses to the Demand Letter. In this draft response, Correia wrote, among other things, that Fraud Guarantee Holdings, LLC “was created as a holding company in February 2016” and that prior Fraud Guarantee entities “were combined into this new holding company, and thus, the members of those entities” became members of the new entity; and that “[s]ignificant dollars were invested into the previous entities.” It does not appear that this draft was sent back to Victim-3's counsel.

s. In or about mid-June 2017, the CEO—having still not been paid for the work he had done since September 2015—separated from Fraud Guarantee.

t. In or about September 2017, the CEO emailed Correia regarding a \$140 fee owed by Fraud Guarantee to its bank, which had gone unpaid since June 2017.

u. On or about September 7, 2017, Correia emailed Victim-1 to request that he “extend [Correia] another \$4,500.” On or about November 6, 2017, Correia emailed Victim-1 to provide him with an update on Fraud Guarantee and to request “a new loan for \$12,000,” for a total loan of \$18,500, which Correia promised to repay with interest “by January 15th, the latest.” Correia stated that such a loan would “relieve one of the ‘business’ concerns that you and I both have had regarding my ability to concentrate fully on Fraud Guarantee. This loan would get me through the next couple months with less stress and time I can devote to getting [an] agreement finalized with the [insurance] carriers.” During this time period, Correia also forwarded Victim-1 various correspondence that Correia was apparently having with certain potential insurance carrier partners. On or about February 6, 2018, Correia emailed Victim-1 to request an additional \$3,500 loan. Correia stated, “I know the company isn’t profitable yet, but, EVEN IF, it takes longer to get the insurance company approval, I am going to move forward with the monitoring product which will be instant revenue and very successful. I just spoke to a family office association and they want to promote it to their entire client base of over 20,000 f[amily] offices as soon as it’s ready. I could do this in 90 days at the most. . . . [T]his will be very profitable.” On or about May 2, 2018, Correia emailed Victim-1 to request “another small loan (\$8500?).” In connection with these various personal loans, Correia agreed to “share with [Victim-1] the proceeds that [Correia] receive[s] from distributions or the sale of .7% of [his] stock, once [he] receive such funds in [his] personal bank account.”

v. In or about late July and early August 2018, Correia informed Victim-1 and Victim-3 that Fraud Guarantee was in discussions with Rudolph Giuliani and his firm, [REDACTED], to enter into some form of business partnership.

w. On or about September 3, 2018, Correia emailed a new potential investor (Victim-4) with the subject line, "Per Lev Parnas": "It was a pleasure meeting you a few weeks ago in New York and I look forward to seeing you again soon. I wanted to congratulate you on joining our team at Fraud Guarantee. . . ." About a week later, Correia emailed Victim-4 to "reach out as we never did connect. We will be finalizing this raise and wanted to reach out to see if you are still interested in participating."

x. On or about September 12, 2018, Correia, copying Parnas, emailed a Fraud Guarantee update to Victim-3 and others. The update stated, among other things, that (i) "we are . . . at the final stages of a viable product," (ii) "we are finalizing a policy with A-rated insurance carriers (via our [REDACTED] partners) that will cover our company through a rather traditional E&O (errors and omissions) insurance policy" and "expect to receive final policy language and pricing, within the next few weeks," (iii) "[w]e have had numerous meetings with Rudy [Giuliani] and his team over the past few months and are in the process of finalizing an agreement with them"; [REDACTED] will provide Fraud Guarantee with a "road map and structure to proactively prevent . . . compliance issues and to properly respond to any inquiries as to our practices," and will "also help open doors to larger institutional clients by working in a business development capacity"; and "Rudy Giuliani is willing to put his name and reputation on the line, personally helping to bring future clients to the table," and (iv) Fraud Guarantee needs to raise an additional "approximately \$5 million to successfully launch our company into the market," including to pay "\$1-\$2M in consulting fees for the first year" to [REDACTED]; and that current

members (including Victim-1) were being offered a “first-right-of-refusal on allocations for this raise.”

y. Following this update, Victim-3 did not learn of any work being performed by Rudolph Giuliani or [REDACTED] in relation to Fraud Guarantee. Nor did Victim-3 learn of Fraud Guarantee entering into any deal with an insurance carrier, bringing any product to market, or otherwise engaging in any business operations.

z. On or about September 19, 2018, Victim-4 transferred \$250,000 to [REDACTED] pursuant to a Note Purchase Agreement with Fraud Guarantee, which provided that Victim-4 was being provided with promissory notes that could convert into Fraud Guarantee equity. Victim-4 understood that this money was covering part of the cost of Fraud Guarantee’s contract with [REDACTED]. On or about October 5, 2018, Victim-4 transferred another \$250,000 to [REDACTED], apparently after Parnas led him to believe that a different potential investor had withdrawn his pledge.

aa. Subsequent to investing in Fraud Guarantee, Victim-4 did not learn of any work being performed by Rudolph Giuliani or [REDACTED] in relation to Fraud Guarantee. Nor did Victim-4 learn of Fraud Guarantee otherwise engaging in any business operations.²

13. Based on my review of materials obtained pursuant to search warrants, in particular search warrants on the iCloud accounts of Parnas, Fruman, and others, which revealed electronic

² According to an October 31, 2019 report in [REDACTED]—which cited “interviews with former business partners, investors and associates of Messrs. Parnas and Correia, as well as company emails, corporate documents and court records”—“[s]ince its inception in 2013, a Florida firm called Fraud Guarantee has attracted no identifiable customers, generated zero returns for investors and—according to Florida court records—defaulted on its office lease years ago after falling behind on rent.”

communications between Parnas and Giuliani (among others),³ I have learned, in substance and in part, that after [REDACTED] was paid \$500,000, ostensibly to retain [REDACTED] consulting services for Fraud Guarantee, it appears that Giuliani principally worked to assist Parnas in his ongoing effort to remove [REDACTED], the then-U.S. Ambassador to Ukraine, from her post. These facts are described at length in the affidavit attached hereto as Exhibit 1 and incorporated by reference herein. *See* Exhibit 1 ¶¶ 44-57.

14. As noted above, Fraud Guarantee's website indicates that the company remains active today. Based on my discussions with the victim-investors and/or their counsel, and the CEO, and my review of documents and financial records, I have learned that, to date, none of the victim-investors has recouped their investments, and that the CEO had not been paid the back-wages he is owed; and that Fraud Guarantee still has no viable products or customers. Further, as reflected in Exhibit 1, Giuliani's work in conjunction with Parnas to remove Ambassador [REDACTED] continued at least through May 2019.

B. Probable Cause Regarding the Subject Accounts

15. Based on the information set forth above, I believe there is probable cause to believe that Parnas, Correia, and others known and unknown engaged in the Subject Offenses by, among other things, inducing and conspiring to induce multiple victims to invest in Fraud Guarantee based on materially false representations about the company, its leadership, and its business partners and prospects. Furthermore, based on the foregoing, the facts set forth below, and my training and experience, there is probable cause to believe that the Subject Accounts will contain evidence and instrumentalities of the Subject Offenses.

³ *See* search warrants and accompanying affidavits marked 19 Mag. 4784 (May 16, 2019); 19 Mag. 9832 (October 21, 2019) (attached hereto as Exhibit 1 and incorporated by reference herein);

16. In particular, the Subject Accounts were used to carry out this fraudulent scheme as Parnas used Subject Account-1 and Correia used Subject Account-2 to engage in communications with each other and with actual and potential victims and business partners in furtherance of the scheme. With respect to Correia, he used Subject Account-2 for virtually all of the communications with Victim-1, Victim-2, Victim-3, Victim-4, Intended Victim-1, and the CEO described above, including multiple communications with each of the actual or potential investors in which Correia transmitted apparently false and baseless representations about the company and its finances, leadership, and relationship with Giuliani and [REDACTED].

17. With respect to Parnas, he appears to have alternated between using Subject Account-1 and a Yahoo account in conjunction with Fraud Guarantee. Among other things, as described above, Parnas used Subject Account-1 to communicate with (i) Victim-1, including on the email in which Victim-1 was sent the Fraud Guarantee loan agreement and the email in which Parnas and Correia determined to cancel that agreement and replace it with an alternative arrangement; (ii) Victim-2, including on the emails in which Victim-2 was sent the Fraud Guarantee purchase agreement and the Operating Agreement reflecting a \$570,000 "capital account" held by Parnas; (iii) Victim-3, including on the email in which Victim-3 was sent the Fraud Guarantee Business Plan containing various apparently false and baseless representations and projections about the company; (iv) Intended Victim-1, including on emails soliciting his investment and sending him the Business Plan; and (v) the CEO, including on emails regarding the CEO's work for Fraud Guarantee and his demand to be paid for back-owed wages.

18. Accordingly, there is probable cause to believe that the Subject Accounts will contain evidence and instrumentalities of the Subject Offenses, including communications with actual or potential investors; communications between Parnas and Correia reflecting the business plans and

operations (if any) of the company; communications with outside parties, such as insurance companies or consultants like [REDACTED], that would shed light on the nature of the company's plans and operations (if any) and/or the scope of the fraudulent scheme or true purpose of the money obtained from investors; and communications with or regarding Giuliani or [REDACTED] which would reveal whether Giuliani was, in fact, performing services for Fraud Guarantee in exchange for the \$500,000 payment to his firm.

19. Furthermore, based on my training and experience, and consistent with the pattern of communications reflected in Exhibit 1, I know that individuals who communicate via text or WhatsApp typically also communicate about the same subjects via email.

20. Additionally, based on my training and experience, email accounts like the Subject Accounts, which have been used to communicate with others in furtherance of the Subject Offenses often contain records of that activity, including email correspondence, address books with contact information for co-conspirators, and documents saved as email attachments or to Google Docs or Google Drive folders.

21. Additionally, based on my training and experience, and my participation in this investigation, it appears that Parnas and Correia had various meetings with actual or potential investors in Fraud Guarantee and with Giuliani, and that evidence in the Subject Accounts will corroborate the existence of such meetings. Specifically, location data, IP transaction records, and calendar entries may contain evidence to establish the location of Parnas, Correia, or others at relevant dates set forth above. Furthermore, device information, and cookie data for linked accounts, may contain evidence of other email accounts or electronic devices that could contain evidence of the Subject Offenses, including correspondence with co-conspirators or location information to corroborate the existence of meetings. Indeed, from my participation in this

investigation, I have learned that the individuals involved in the commission of the Subject Offenses have used multiple email or iCloud accounts, and/or multiple cellphones, to communicate with co-conspirators.

22. Temporal Limitation. This application is limited to all content created, sent, or received on or after September 1, 2013, which is shortly before Fraud Guarantee was registered in Delaware, to the present.

C. Evidence, Fruits and Instrumentalities

23. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

24. In particular, I believe the Subject Accounts are likely to contain the following information:

- a. Evidence relating to, including communications with, Rudolph Giuliani, [REDACTED] and any actual or potential investors, members, or partners of Fraud Guarantee;
- b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;
- c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;
- d. Evidence relating to false and fraudulent representations made to potential or actual investors, including drafts of any corporate documents and related materials;
- e. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

f. Evidence relating to the nature and extent of Rudolph Giuliani's and [REDACTED] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [REDACTED] and whether or not such efforts benefited Fraud Guarantee;

g. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

h. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

i. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

j. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

k. Passwords or other information needed to access user's online accounts.

III. Review of the Information Obtained Pursuant to the Warrant

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts

under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

26. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

27. While Parnas, Correia, and others have been publicly indicted with respect to separate charges, and there has been some public reporting about the existence of an investigation into the removal of Ambassador [REDACTED], the scope and focus of this aspect of the criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert criminal targets to the scope and focus of the investigation, causing them to destroy evidence, tamper with witnesses, or otherwise seriously jeopardize the

investigation. Specifically, from my experience investigating public corruption offenses, I know that individuals who participate in offenses such as the Subject Offenses may communicate about known government investigations and tailor their stories to be consistent, and tamper with or hide potential evidence. Accordingly, premature disclosure of the scope of this investigation would undermine efforts to obtain truthful statements from relevant witnesses, and could lead to witness tampering and/or obstruction of justice. In addition, if the subjects of this investigation were alerted to the existence of a criminal investigation, it may prompt them to delete electronic records,

including in e-mail accounts or other electronic media not presently known to the government. Accordingly, there is reason to believe that, were the Provider to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized.

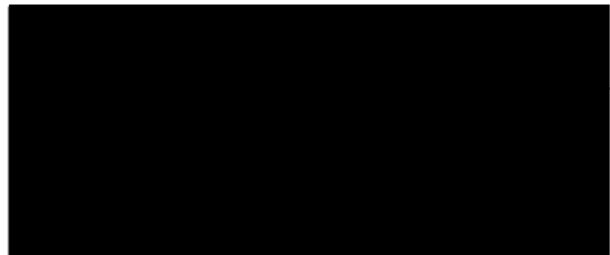
28. Additionally, while the Subject Accounts are registered to an enterprise domain (fraudguarantee.com), there is no representative of the enterprise that could be notified without seriously jeopardizing the investigation. Indeed, as described above, the subscribers of the Subject Accounts are the CEO and COO of the enterprise, the enterprise itself appears to be an instrumentality of the fraudulent scheme, and there is no known employee of the enterprise or a legal representative that could be notified without jeopardizing the investigation. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person, including any representative of the enterprise domain fraudguarantee.com, of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

29. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as

need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

30. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.



Sworn to before me this
12th day of December, 2019

A handwritten signature in black ink, appearing to read "J. Paul Oetken", written over a horizontal line.

HONORABLE J. PAUL OETKEN
United States District Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

19 MAG 11651

In the Matter of a Warrant for All
Content and Other Information
Associated with the Email Accounts
and

Maintained at Premises Controlled by
Google, LLC, USAO Reference No.
[REDACTED]

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, LLC ("Provider")

Federal Bureau of Investigation and United States Attorney's Office for the Southern
District of New York

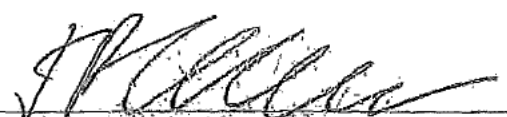
1. **Warrant.** Upon an affidavit of Special Agent [REDACTED] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [REDACTED] and [REDACTED], maintained at premises controlled by Google, LLC, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, and/or tampering with potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person, including but not limited to a representative of the enterprise domain, for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

Dec. 12, 2019 3:03 PM
Date Issued Time Issued


HONORABLE J. PAUL OETKEN
United States District Judge
Southern District of New York

Email Search Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Google, LLC (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts [REDACTED] and [REDACTED] (the "Subject Accounts"). The Provider is directed to produce the information described below associated with the Subject Accounts, limited to content created, sent, or received on or after September 1, 2013 through the date of this warrant.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts (subject to the time period limitation set forth above):

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Google Drive Content.* All Google Drive records associated with the Subject Accounts, including all documents and other records stored on the Google Drive accounts.

f. *Google Docs.* All Google Docs records associated with the Subject Accounts, including all documents created or stored in Google Docs.

g. *Google Calendar.* All calendar entries and records associated with the Subject Accounts.

h. *Location History.* All location records associated with the Subject Accounts.

i. *Information Regarding Linked Accounts, Including Accounts Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Accounts, including specifically by Cookie, email account, phone number, Google Account ID, Android ID, or other account or device identifier.

j. *Device Information.* Any information identifying the device or devices used to access the Subject Accounts, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber

Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access the Subject Accounts;

k. *Android Services*. All records relating to Android services associated with the Subject Accounts.

l. *Preserved or backup records*. Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (the "Subject Offenses"), including the following:

- a. Evidence relating to, including communications with, Rudolph Giuliani, [REDACTED], and any actual or potential investors, members, or partners of Fraud Guarantee;
- b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;
- c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;
- d. Evidence relating to false and fraudulent representations made to potential or actual investors, including drafts of any corporate documents and related materials;
- e. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

f. Evidence relating to the nature and extent of Rudolph Giuliani's and [REDACTED] [REDACTED] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [REDACTED] and whether or not such efforts benefited Fraud Guarantee;

g. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

h. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

i. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

j. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

k. Passwords or other information needed to access user's online accounts.

Exhibit 1

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)the Contents of Four iCloud Accounts Currently Located
on a Hard Drive Containing the Results of A Prior iCloud
Search Warrant

19 MAG 9832

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Southern District of New York
(Identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property
to be seized):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.**YOU ARE COMMANDED** to execute this warrant on or before November 4, 2019

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court.JPO
USMJ Initials☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☒ for 30 days (not to exceed 30).☐ Until, the facts justifying, the later specific date of _____

Date and time issued:

Oct. 21, 2019
10:38 a.m.

Judge's signature

City and state: New York, New YorkJ. Paul Oetken, United States District Judge

Printed name and title

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized:		
<p style="text-align: center;">Certification</p> <p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.</p> <p>Date: _____</p> <p style="text-align: right;">_____ <i>Executing officer's signature</i></p> <p style="text-align: right;">_____ <i>Printed name and title</i></p>		

Attachment A

I. Device to be Searched

The device to be searched (the "Subject Device") is described as a hard drive containing the contents of the below four iCloud accounts, which were obtained pursuant to a search warrant authorized on or about May 16, 2019, by the Honorable Stewart Aaron, Magistrate Judge for the Southern District of New York, criminal number 19 Mag. 4784:

<i>iCloud Account</i>	<i>Owner</i>	<i>Referred To As</i>
[REDACTED]	Lev Parnas	Subject Account-1
[REDACTED]	Lev Parnas	Subject Account-2
[REDACTED]	Igor Fruman	Subject Account-3
[REDACTED]	[REDACTED]	Subject Account-4
(collectively, the "Subject Accounts")		

II. Review of ESI on the Subject Device

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Accounts for evidence, fruits, and instrumentalities of one or more violations of 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); and 18 U.S.C. § 1343 (wire fraud) (together, the "Subject Offenses"), as listed below:

- a. Evidence related to any false statements or documents made or caused to be made to the Federal Election Commission.
- b. Evidence relating to the May 9, 2018 letter from Congressman [REDACTED] to Secretary of State [REDACTED] regarding U.S. Ambassador [REDACTED], including correspondence attaching or concerning the letter.
- c. Communications with individuals associated with the government or a political party in the Ukraine, including [REDACTED].
- d. Communications regarding [REDACTED] specifically or the position of U.S. Ambassador to Ukraine generally.
- e. Evidence, including travel records, related to meetings with Ukrainian government officials involving Rudolph Giuliani, [REDACTED], Parnas, or Fruman.
- f. Evidence of knowledge of the foreign agent registration laws and requirements, or lobbying laws, including but not limited to knowledge of the requirement to register as an agent of a foreign principal, or of the prohibition of acting on behalf of, lobbying for, or making contributions on behalf of a foreign principal.

g. Evidence of the intent of Parnas, Igor Fruman, [REDACTED], David Correia, .
Andrey Kukushkin, Andrey Muraviev, Giuliani, [REDACTED] as it
relates to the Subject Offenses under investigation.

AO 106 (SDNY Rev. 01/17) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 the Contents of Four iCloud Accounts Currently
 Located on a Hard Drive

19 MAG 9832
Case No.

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)

Offense Description(s)

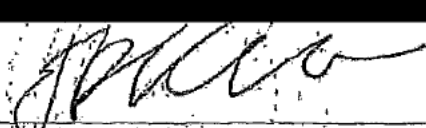
See Attachment A

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 10/24/2019City and state: New York, New York

 Judge's signature

J. Paul Oatken, United States District Judge

Printed name and title

19 MAG 9832

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search Warrant for the Contents of Four iCloud Accounts Currently Located on a Hard Drive Containing the Results of A Prior iCloud Search Warrant, USAO Reference No [REDACTED]

TO BE FILED UNDER SEAL

Agent Affidavit in Support of
Application for a Search Warrant

SOUTHERN DISTRICT OF NEW YORK ss.:

[REDACTED], being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence, including emails.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search four iCloud accounts on the electronic device specified below (the "Subject Device") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and

conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. Prior Warrants and Subject Device

3. On or about January 18, 2019, the United States Attorney's Office for the Southern District of New York ("USAO") and FBI sought and obtained from the Honorable Sarah Netburn, Magistrate Judge for the Southern District of New York, a search warrant (the "January 18 Warrant"), criminal number 19 Mag. 729, for email accounts belonging to Lev Parnas, Igor Fruman, David Correia, and [REDACTED], among others.

4. On or about October 17, 2019, the USAO sought and obtained from the Honorable J. Paul Oetken, United States District Judge for the Southern District of New York, a warrant, criminal number 19 Mag. 7595, for the January 18 Warrant returns.¹

5. On or about May 16, 2019, the USAO and FBI sought and obtained from the Honorable Stewart Aaron, Magistrate Judge for the Southern District of New York, a search warrant (the "May 16 Warrant"), criminal number 19 Mag. 4784, for the following iCloud accounts:²

¹ On August 14, 2019, the USAO and FBI sought a warrant from the Honorable Henry B. Pitman, Magistrate Judge for the Southern District of New York, to conduct an expanded search of the January 18 Warrant returns. Judge Pitman reviewed and approved the application, and both the affiant and Judge Pitman signed the affidavit in support of the application for a warrant, which was assigned docket number 19 Mag. 7595. However, at present, the Government is unable to locate a copy of the search warrant, which, to the extent it was presented to Judge Pitman, was not retained. Accordingly, on October 17, 2019, the USAO presented the signed copy of the 19 Mag. 7595 application to Judge Oetken, who, that same day, issued a new warrant authorizing the seizure of the same materials sought in the August 14 application. Moreover, no material identified herein was seized pursuant to the August 14 application. All of the material discussed herein that is attributed to the January 18 Warrant was seized and identified pursuant to that original judicial authorization.

² Based on my review of the iCloud account returns obtained pursuant to the May 16 Warrant, which is still ongoing, I understand that Parnas stored relevant text messages (including iMessages sent from an iPhone) and photos, among other materials, on Subject Account-1; that Parnas stored

<i>iCloud Account</i>	<i>Owner</i>	<i>Referred To As</i>
[REDACTED]	Lev Parnas	Subject Account-1
[REDACTED]	Lev Parnas	Subject Account-2
[REDACTED]	Igor Fruman	Subject Account-3
[REDACTED]	[REDACTED]	Subject Account-4
(collectively, the "Subject Accounts")		

6. With respect to the May 16 Warrant, Judge Aaron directed Apple to provide content and other information for the iCloud accounts in the chart below to search for evidence of violations of 52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful foreign contributions), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statements in a matter within the jurisdiction of the executive branch), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1346 (honest services fraud), and 18 U.S.C. § 1956 (money laundering) (together, the "May 16 Warrant Subject Offenses").

7. The Subject Device is particularly described as a hard drive in the possession of the FBI which contains the results of the May 16 Warrant for the Subject Accounts. Apple provided the content and information responsive to the May 16 Warrant electronically, which was downloaded by the FBI onto the Subject Device. As detailed herein, by this application, the

relevant text messages (including iMessages sent from an iPhone), WhatsApp messages, and photos on Subject Account-2, and that Fruman stored relevant documents on Subject Account-3. While my review of Subject Account-4 has not yet begun, based on my review of materials obtained pursuant to the May 16 Warrant for Subject Account-2, I have learned that [REDACTED] used the phone associated with Subject Account-4 to exchange relevant messages and emails with Parnas regarding the Subject Offenses. Thus, for the reasons discussed herein, there is probable cause to believe that evidence of the Subject Offenses, in addition to evidence of the May 16 Warrant Offenses, will be found on the Subject Accounts.

Government seeks authorization to expand the scope of its search of the iCloud accounts contained on the Subject Device.³

8. On October 9, 2019, a grand jury sitting in the United States Attorney's Office for the Southern District of New York returned an indictment charging (i) Lev Parnas and Igor Fruman with conspiring to make unlawful straw donations, making and willfully causing false statements to be made to the FEC, and fabricating documents to impede, obstruct, and influence the proper administration of a matter within the FEC's jurisdiction, in violation of 52 U.S.C. §§ 30122 and 18 U.S.C. §§ 371, 1001, 2, and 1519; and (ii) charging Lev Parnas, Igor Fruman, David Correia and Andrey Kukushkin with conspiring to make unlawful foreign contributions in violation of 52 U.S.C. § 30121 and 18 U.S.C. § 371.

C. The Subject Offenses

9. In the course of reviewing the content contained on the Subject Accounts for evidence of the May 16 Warrant Subject Offenses, I have discovered materials which, as set forth in greater detail below, establish probable cause to believe the Subject Accounts contain evidence of additional offenses. I am therefore requesting authority to search the Subject Device for evidence, fruits, and/or instrumentalities of these additional offenses.

10. In particular, I respectfully submit that there is probable cause to believe that the Subject Accounts on the Subject Device also contain evidence, fruits, and/or instrumentalities of the commission of one or more of the following: 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); and 18 U.S.C. § 1343 (wire fraud) (together, the "Subject Offenses").

³ A filter team comprised of Assistant United States Attorneys and FBI agents who are not a part of the prosecution team have used search terms to separate any potentially privileged documents out of the shared database to which the prosecution team has access.

II. Probable Cause Regarding the Subject Offenses

11. The FBI and the USAO-SDNY are investigating, among other things discussed herein, schemes involving Lev Parnas, Igor Fruman, David Correia, Andrey Kukushkin and others to make political contributions to candidates and political action committees ("PACs") in order to gain access to politicians and influence policy, in violation of certain of the Subject Offenses. First, there is probable cause to believe that Parnas made illegal "straw donations," funded by third parties, in violation of the federal campaign finance laws, which prohibit persons from making contributions in the name of another person, and caused false forms to be submitted to the FEC. See 18 U.S.C. § 1001, 1519, and 2, 52 U.S.C. § 30122. Some of those contributions were made in the name of Global Energy Producers LLC ("GEP"), a purported liquefied natural gas ("LNG") import-export business that had been incorporated by Igor Fruman and Parnas around the time the contributions were made.⁴ The rest of the contributions were made in the names of Igor Fruman and Parnas, although, as discussed below, Igor Fruman paid for Parnas's contributions. Second, in 2018, it appears that Parnas, Igor Fruman, Correia, Andrey Muraviev, and Kukushkin conspired to attempt to acquire cannabis licenses in multiple states by, among other things, donating to politicians in those states. Members of the group hired lobbyists, Correia identified the specific contributions the group should make in order to obtain licenses, and Muraviev – a Russian national with no legal status in the United States – wired \$1 million from overseas to the United States, some of which was used to make contributions to politicians in Nevada and elsewhere, in violation

⁴ Two of the contributions funded by Fruman and effectuated by Parnas were made in the name of GEP, which, as described below, appears to be a corporation created at or shortly before the time the contributions were made for the principal purpose of obscuring the true donor's identity. The FEC has interpreted the so-called straw donor prohibition as not only applying to individuals, but also to the creation and use of closely held corporations or corporate LLCs for the purpose of concealing the true source of the funds.